9.8.2025: Math 122 Lecture 2 Notes

Vasily Krylov

1 Last Time

Last time we established the notion of a group, given by a set and law of composition (S, m). A group must satisfy the following axioms;

- **Identity:** It must contain the identity element, $e \in S$
- **Inverse:** Each element must have an inverse in the group; $\forall b \in S, \exists b^{-1} \in S : bb^{-1} = e$
- **Associativity:** For elements $a, b, c \in S$, we must have that $(ab)c = a(bc)$.

Some common examples of groups are: $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}/n\mathbb{Z}, +)$.

Monoid: A monoid satisfies the first and third axiom, but does not have an inverse for every element. We can however establish a group, S^x. For example, $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}, \mathbb{R}^\times = \mathbb{R}\backslash\{0\}, \mathbb{C}^\times = \mathbb{C}\backslash\{0\}$.

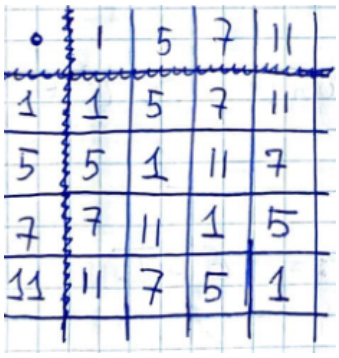
What about $(\mathbb{Z}/n\mathbb{Z})^\times$? We can first guess $(\mathbb{Z}/n\mathbb{Z})^\times) = \{1, 2, \cdots, n-1\}$. For example, $n = 3 \implies (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$ with inverses $1^{-1} = 1$ and $2^{-1} = 2$.
For $n = 4$, we have $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$. See the corresponding Cayley Table below

•	1	2	3	
1	1	2	3	
2	2	0	2	
3	3	2	1	

For $n = 9$, we see that $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$, and also see the corresponding Cayley Table.

Exercise: $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \{1, \cdots, n-1\}; \gcd(a, n) = 1\}$.

Other examples include $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$ and $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. See the corresponding Cayley Table.



For p prime, then we have that $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \cdots, p-1\}$

All of the groups we have covered so far have been commutative (abelian). That is, for any two elements $a, b \in S$, then $ab = ba$. Now let's construct our first example of a non-commutative group.

2 Group of Permutations:

Let T be a nonempty set;

$$S_T := \{\sigma : T \to T | \sigma \text{ bijective}\}$$

We can multiply permutations $\sigma \cdot \tau := \sigma \circ \tau$, where for $t \in T$ we have $t \to \sigma(\tau(t))$.
We claim that $(S_T, \cdot)$ is a group.

Proof: (i) Identity. e is the permutation id_T that sends $t \to t$.

(ii) Inverse: start with $\sigma : T \to T$, where σ sends $a \to b, c \to d, e \to f, \cdots$, then σ^{-1} sends $b \to a, d \to c, f \to e, \cdots$ (reversing the arrows). More formally, for $t \in T$, $\sigma^{-1}(t) = s$ such that $\sigma(s) = t$, Such an s exists implies σ is surjective, and if it is unique then σ is injective.
(iii) Associativity: $(\sigma \circ \tau) \circ f =? \sigma \circ (\tau \circ f)$. Both of them are given by $t \to \sigma(\tau(f(t)))$. Indeed:

$$((\sigma \circ \tau) \circ f)(t) = (\sigma \circ \tau)(f(t)) = \sigma(\tau(f(t))) = \sigma((\tau \circ f(t))) = (\sigma \circ (\tau \circ f))(t)$$

Thus completing the proof that this is a group.

Now assume that T is finite. We can identify $T = \{1, 2, \cdots, n\}$, and $S_{\{1,2,\cdots,n\}}$ is the group of permutations of indices $1, \cdots, n$, denoted by S_n and known as the *symmetric group*. $\sigma \in S_n$ can be written as;

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

For example; $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ sends $1 \to 3, 2 \to 1, 3 \to 2$.
An extremely useful way of writing permutations is using cycle notation. Using our last example, we can view this as $1 \to 3 \to 2 \to 1$, forming a cycle. We will use the following notation; (132) sends 2 to 1, 1 to 3, and 3 to 2. More generally, we can write $(a_1 \cdots a_n$ to send $a_1 \to a_2, a_2 \to a_3, \cdots, a_n \to a_1$.

Permutations may contain more than one cycle. For example; $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}$ contains the cycle $1 \to 4 \to 1$, as well as the cycle $2 \to 5 \to 3 \to 2$, so that we can write $\sigma = (14)(253)$.

Claim: Every permutation σ can be written in cycle notation.

Remarks:
1. Cycle notation IS NOT unique. For example, $(253) = (325) = (532)$ all represent the cycle $2 \to 5 \to 3 \to 2$. Also, the elements (14) and (253) commute, $(14)(253) = (253)(14)$.
2. It is very convenient to omit 1-cycles from the notation. For example; $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ in cycle notation is (13)(2), but we simply write it as (13). The only exception is the identity permutation; $\begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{bmatrix}$ which we denote by 1.

WARNING: (12) may refer to both; $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \in S_2$ or $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \in S_3$

2.1 Product in Cycle Notation

The product $\sigma \circ \tau$ means "do τ first, and then do σ". For example;

$$(1452) \circ (341)(25) = 135$$

$$\begin{gathered} 1 \to^{\tau} 3 \to^{\sigma} 3 \\ 3 \to^{\tau} 4 \to^{\sigma} 5 \\ 5 \to^{\tau} 2 \to^{\sigma} 1 \\ 2 \to^{\tau} 5 \to^{\sigma} 2 \\ 4 \to^{\tau} 1 \to^{\sigma} 4 \end{gathered}$$

Noting that the first three rows give (135), while the bottom two are the one cycles (2) and (4).
Exercise: Show that $(341)(25) \circ (1452) = (234)$. We see that $\sigma \circ \tau \neq \tau \circ \sigma$, so S_5 is NOT commutative (non-abelian).

The group S_n has $n! = n(n-1)\cdots(2)(1)$ elements. Let's consider $n = 3$ in more detail

2.2 Group $\mathbf{S_3}$

Let's describe explicitly the group S_3. Set;

$$x := (123);\ y := (12)$$

We have:

$$x^3 = 1,\ y^2 = 1,\ yx = x^2y (*)$$

which are relations between the elements. Note that $(12)(123) = (1)(23) = (132)(12)$. We can represent the elements as;

$$S_3 = \{1, x = (123), x^2 = (132), y = (12), xy = (13), x^2y = (23)\}$$

Therefore we can say that S_3 is the group generated by x, y subjected to the relations $(*)$.

For example, if we want to compute;

$$xy \cdot x^2y = xyx^2y = xyxxy = x^3yxy = yxy = x^2y^2 = x^2$$

We also see that S_3 is not commutative;

$$yx = x^2y \neq xy$$

since $x^2y = (23)$ and $xy = (13)$.

Exercise: If S is a group that contains less than 6 elements, then S is commutative.
Therefore we see that S_3 is the "smallest" non-commutative group.